DOCUMENT RESUME

ED 398 919 IR 055 977

AUTHOR Siders, Bill
TITLE Open Internet Access in a Structured School Environment: "Controlling Chat Lines During Study Hall."
PUB DATE 95
NOTE 7p.; In: The Internet--Flames, Firewalls and the Future. Proceedings for the 1995 Conference of the Council for Higher Education Computing Services (CHECS) (Roswell, New Mexico, November 8-10, 1995).
PUB TYPE Reports - Evaluative/Feasibility (142) -- Speeches/Conference Papers (150)

EDRS PRICE MF01/PC01 Plus Postage.
DESCRIPTORS *Access to Information; Computer Mediated Communication; Computer Networks; Computer Terminals; Computer Uses in Education; *Educational Policy; *Eligibility; Internet; *Military Schools; Problems; Secondary Education; Study; Two Year Colleges; *Users (Information)
IDENTIFIERS *Academic Computing; Age Appropriateness; Computer Services; Computer Use; New Mexico; Restrictive Procedures

ABSTRACT

At the New Mexico Military Institute (NMMI), both a four-year high school and a two-year junior college, students spend weekday evenings at their desks in mandatory study hall. The goal of NMMI for its campus network is to have a network tap on the desk of each cadet (as well as faculty and administrative staff). The Internet, now already implemented, is an open structure with little or no control placed on access, and this posed a problem at the Institute because of the wide variety of ages of cadets attending the school. This paper describes the types of accessible services, modes of access, and the challenge of programming a security front end which selectively restricts Internet use based on time of the day, day of the week, student class rank, grade point average (GPA), deportment, and other factors. The security system also makes it possible to restrict certain Internet privileges (Telnet and e-mail) on an individual basis. An Internet database (in POISE DMS format) holds all relevant data. Selected individuals may update the database on demand to change access restrictions. (Author/SWC)

OPEN INTERNET ACCESS IN A STRUCTURED SCHOOL ENVIRONMENT

"Controlling Chat Lines During Study Hall"

by: Bill Siders,
Computer Services
New Mexico Military Institute
Roswell NM 88201

ABSTRACT

The New Mexico Military Institute is a unique school in many ways. NMMI is a 4 year high school--2 year junior college with a strong emphasis on academic preparation and excellence, a strong student leadership program, and a highly structured student life. At 7:00 P.M. every weekday evening the entire student body is at a desk with open book ready for Night Study Hall. By 11:00 P.M. all students are in bed for lights out and sleep. At 5:30 the next morning they are up preparing for the day's activity.

Another unique aspect of the Institute is the campus network. The goal is a network tap on the desk of each cadet, faculty, or administrative staff. Last January, the Internet became part of the campus network. The Internet by design is an open structure with little or no control placed on access. This posed a serious problem at the Institute. What is appropriate for a 23 year old college sophomore may not be appropriate for a 14 year old high school freshman. How can the Internet be available to cadets at their desk, yet restricted based on time of the day, class, GPA, deportment, etc.?

Currently all cadet access to the Internet is through the VAX cluster by way of TGV's Multinet. Multinet provides eMail, Telnet, FTP, TCP/IP, Finger, Ping and SNMP. VMS freeware from various Internet sites provide other Internet utilities, Gopher, a Web client (Lynx), and Hytelnet. The cadet has access to a full set of Internet utilities while providing Computer Services' staff VMS protection and programming tools to control access.

NMMI Computer Services has programmed a security front end (based on VMS security features) to control access to Internet utilities based on time of day, day of week, student class rank, GPA, and deportment. It is also possible to restrict certain Internet capabilities (Telnet and eMail) on an individual basis. An Internet database (in POISE DMS format) holds all relevant data. Selected individuals may update the database on demand to change access restrictions.

PROBLEM

NMMI is 3 years into an ambitious project to provide network access to all cadets at the barracks desktop. Network access currently is serial access for PC's, Macintosh and terminals. TCP/IP will be available next year with completion of the Saunders project. Thanks to generous funding from the NMMI Foundation, cadets may lease terminals at nominal cost for basic network access. Currently 36% of the corps are active computer users with only one of the two barracks on the campus network.

The vision for cadet access sees the work station screen (PC, Mac or terminal) as a window into information systems, local and international. Menu driven interfaces provide cadet access to Institute data bases, general campus information, the campus on-line public catalog, a spreadsheet, text processing, email, and printing capability. Wide area access was added spring semester 1995 when NMMI joined CHECSNet and the Internet. Initial costs for the Internet connection are covered by an NSF grant administered by ENMU Portales. Cadet reaction to Internet access was enthusiastic, particularly email and chat lines.

A large percentage of cadets are from out of state and a significant number of cadet families have access to Internet. In addition a number of cadets have accounts at university computer centers around the nation. The enthusiasm was so high that some cadets were on the computer all night raising serious concerns among faculty and staff, particularly for high school age cadets. While the situation was viewed with alarm by some faculty and administrators, the Commandant saw the issue providing an excellent opportunity to teach responsibility. Internet access is not a right but a privilege to be earned and used responsibly.

COMMANDANT'S RULES FOR INTERNET ACCESS

During spring semester of 1995, meetings were held with the Commandant on the parameters to use in restricting cadet internet access. Chat lines and email during night study hall are the major concerns. The intent is not to block access to the Internet for use as a reference but to limit "chatting". Since most chat lines use Telnet for access, limiting Telnet and email were deemed sufficient. Even access to chat lines via Gopher or Lynx makes a Telnet connection using the foreign command TELNET. The Commandant established the following definitions for cadet access and published them in the Cadet Blue Book of Regulations:

A. No RAT (Recruit At Training) will have access to the Internet at any time for the first 3 weeks.

B. Upon completion of the first 3 weeks, RAT's will have access to Internet mail and Telnet during non-study hall times but will only have access to Internet for NSH.

C. Cadets on academic or disciplinary probation will be restricted from the use of Internet mail and Telnet during NSH.

D. Cadets with less than a 2.0 cumulative GPA or less than a "C" in deportment will be restricted from the use of Internet mail and Telnet during NSH.

E. All 4th, 5th, and 6th class cadets, regardless of status, will be restricted from the use of Internet mail and Telnet during NSH and from Telnet at all times.

F. All 1st, 2nd and 3rd class yearlings or old cadets will be authorized full access at any time unless they fall under paragraph c or d above.

A data file was created in the POISE DMS format and entry screens prepared. A sample screen follows:

Internet Restriction file - Commandant's Office

==========

Cadet Number _____ UserName _____

Data from CMD$DATA:INFO

Cadet Data
Academic Class: ____
Cumulative GPA: ____
Status __
Probation
Academic: ___
Disciplinary: ___

Restrictions	Full Time	NSH Only
Internet:	___	___
Mail:	___	___
Telnet:	___	___

Flag Fields in Cadet Internet
RAT (Y/N) ___
Commandant's Override ___

Restrictions above are set nightly based upon flags to the left.

Possible restriction flags are
blank = no restriction.
Y = cadet is restricted.
P = permanent restriction, added and removed by operator.

Each night a system procedure loads the cadet ID number and account username from the system authorization tables. It then loads data from the Commandant's information file into Academic Class, Cummulative GPA, Status, Academic Probation, and Disciplinary Probation. A short program then uses the flag fields just set, to calculate the restriction flags. If the restriction field currently holds a blank or "Y", a new value overwrites the old. If the restriction field holds a "P", no changes are made. Control of access restrictions is provided by another program.

COMPUTER CONSIDERATIONS

The Digital VAX VMS file protection scheme is based upon four groups of users (System, Owner, Group, and World). The System group is any system user or anyone possessing the privilege SYSPRV. The Owner group is the owner of the file in question. The group designated as Group is based upon the UIC (User Identification Code) of VMS. It is any user holding the same UIC class. The World category is any other user on the system.

Four possible access modes (Read, Write, Execute, Delete) are also available in Digital's file protection scheme. Read access allows the user to read the file in question. Write access allows the user to write to the file. Execute allows execute access to compiled images. Delete allows the user to remove the file from the system. Thus a typical protection mask is (S:RWED,O:RWED,G:R,W). System has read, write, execute and delete access as does the owner. Members of the same group have read access only and others on the system have no access.

An additional protection scheme is available within VMS through the use of ACL's (Access Control Lists). A system level user may create an identifier which is recognized by all levels of the file system. The system user then grants the identifier to a single user or group of users. It is analogous to a key to allow entry to the file system. An ACL is then placed on a file or device granting levels of access for holders of a particular identifier. The ACL is equivalent to a file lock granting access to holders of the correct key. ACL's provide a great deal of flexibility in granting access to various files.

Identifiers are granted within the user authorization process and are normally permanent qualities of a user account. A super user, one with the privilege CMKRNL, may however grant or revoke an identifier on the fly. This is the basis of the NMMI Cadet Internet Restriction procedure.

LOGIC OF INTERNET RESTRICTION SYSTEM

All cadets at NMMI have a computer account with username CADETnnnnnn where nnnnnn is the cadet's ID number. This allows utilities written at NMMI to read the username and from it parse the cadet's ID number. This in turn provides key access into the Institute databases. Each such account holds the identifier CADET as a permanent aspect of the account. Many programs, procedures, data files, and disks have the ACL

(IDENT=CADET, ACCESS=NONE).

This limits cadet access to the file system. A similar ACL is placed on all Internet utilities blocking cadet access. An additional identifier, INTERNET, is placed on all Internet utilities so that the INTERNET identifier precedes the CADET identifier. For example:

```
GOPHER.EXE;4   [SYSTEM,SIDERSB]   (RWED,RWED,RE,RE)
(IDENTIFIER=INTERNET,ACCESS=READ+EXECUTE)
(IDENTIFIER=CADET,ACCESS=NONE)
```

The GOPHER utility has a protection mask

(S:RWED,O:RWED,G:RE,W:RE)

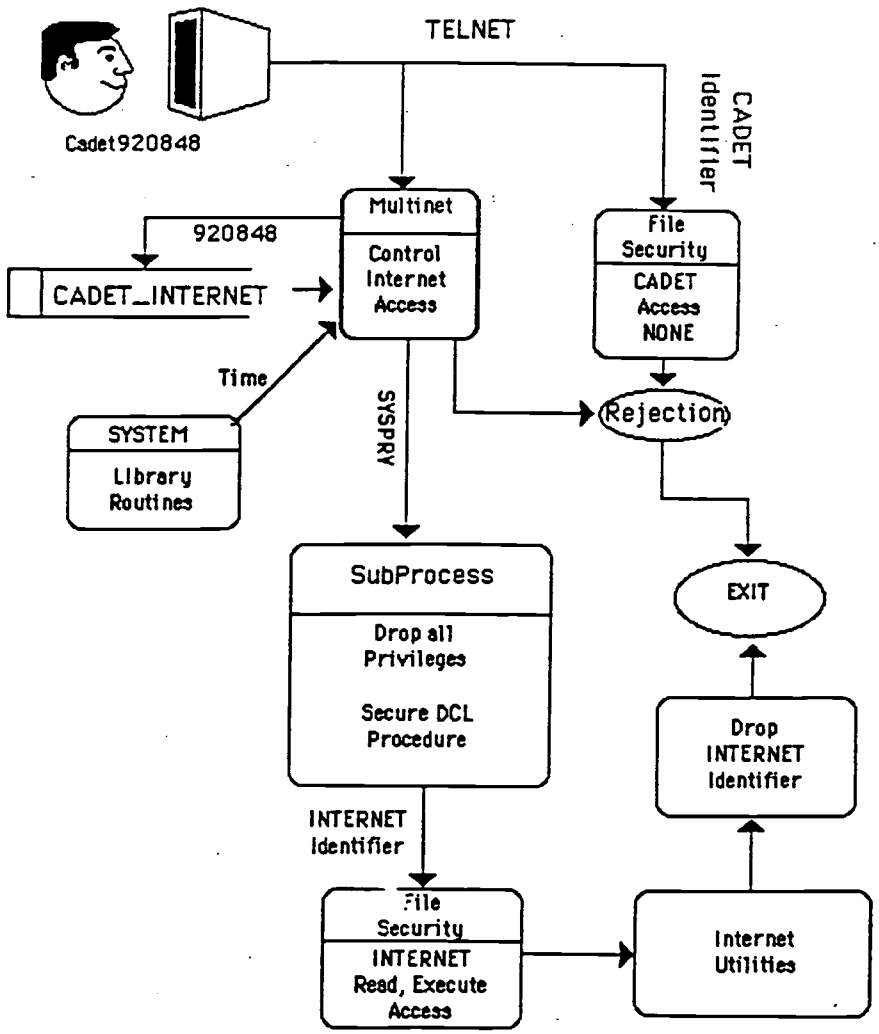
which allows anyone on the NMMI cluster to access the utility. Cadets however (holders of the identifier CADET) are restricted by that ACL. If the cadet is granted the identifier INTERNET, that ACL takes precedent and the GOPHER utility may be executed.

A BASIC program grants the identifier INTERNET to cadets under specified conditions. The program is installed with SYSPRV, SETPRV, and CMKRNL. SYSPRV allows access to files normally not available to the cadet. SETPRV allows the program to assume or drop privileges and CMKRNL allows the program to grant and revoke the identifier INTERNET. The program is defined as a foreign command and parses parameters passed at execution. That is, the command GOPHER is replaced by INTERNET GOPHER where INTERNET is NMMDISK:[MULTINET]MULTINET.EXE.

The program

- parses the passed parameters.
- reads system time and determines if its Night Study Hall.
- reads the Username and parses cadet ID.
- checks the data file for restrictions on the cadet.
- spawns a subprocess to execute a secure DCL procedure if appropriate.

The spawned subprocess drops all privileges associated with the parent process. The cadet executes the Internet utilities without privileges. If restrictions are in place on the cadet, a message is displayed informing the cadet of the fact, and the identifier is not granted. If no restrictions are in place on the requested utility, the program grants the identifier and spawns a subprocess to execute the secure DCL procedure. Since the program has SYSPRV it may execute the procedure where the cadet may not. Once the subprocess assumes control, privilege is dropped and the cadet executes the Internet utility via the ACL. This avoids the problem of allowing the cadet to execute an Internet utility like GOPHER, while holding exceptional privilege.



Other Applications

The use of the cadet's username to arrive at a cadet ID number which in turn provides access to the tabled restrictions in the data file, is more an artifact of existing username structure than a requirement for this application. One could use the VMS account username as the key for the restrictions file as well. Rather than placing restrictions, procedure or program names and accompanying identifiers may be tabled in the data file. For example:

Username	Procedure	Identifier	Procedure	Identifier
SIDERSB	GYM-Billing	GDYBIL	AR-CleanUp	AR
TODD	GOLF-Billing	GLFSYS	GOLF-REG	GLFSYS

A use of VMS protection and ACL's similar to that above, will then provide read or write access to data files on a procedure by procedure basis. For example a user in one office may be granted an identifier allowing update of data files across data bases in several other offices; all in a highly controlled and transparent fashion.

U.S. Department of Education
Office of Educational Research and Improvement (OERI)
Educational Resources Information Center (ERIC)

REPRODUCTION RELEASE

(Specific Document)

I. DOCUMENT IDENTIFICATION:

Title:
"THE INTERNET - FLAMES, FIREWALLS AND THE FUTURE"
ANY FUTURE PROCEEDINGS FROM THE CHECS CONFERENCES

Author(s): VARIOUS

Corporate Source:
CHECS

Publication Date:
FALL 1995
EVERY FALL

II. REPRODUCTION RELEASE:

In order to disseminate as widely as possible timely and significant materials of interest to the educational community, documents announced in the monthly abstract journal of the ERIC system, *Resources in Education* (RIE), are usually made available to users in microfiche, reproduced paper copy, and electronic/optical media, and sold through the ERIC Document Reproduction Service (EDRS) or other ERIC vendors. Credit is given to the source of each document, and, if reproduction release is granted, one of the following notices is affixed to the document.

If permission is granted to reproduce and disseminate the identified document, please CHECK ONE of the following two options and sign at the bottom of the page.

	The sample sticker shown below will be affixed to all **Level 1** documents	The sample sticker shown below will be affixed to all **Level 2** documents	
[X] Check here **For Level 1 Release:** Permitting reproduction in microfiche (4" x 6" film) or other ERIC archival media (e.g., electronic or optical) *and* paper copy.	PERMISSION TO REPRODUCE AND DISSEMINATE THIS MATERIAL HAS BEEN GRANTED BY Sample TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)	PERMISSION TO REPRODUCE AND DISSEMINATE THIS MATERIAL IN OTHER THAN PAPER COPY HAS BEEN GRANTED BY Sample TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)	[ ] Check here **For Level 2 Release:** Permitting reproduction in microfiche (4" x 6" film) or other ERIC archival media (e.g., electronic or optical), but *not* in paper copy.
	Level 1	Level 2	

Documents will be processed as indicated provided reproduction quality permits. If permission to reproduce is granted, but neither box is checked, documents will be processed at **Level 1**.

"I hereby grant to the Educational Resources Information Center (ERIC) nonexclusive permission to reproduce and disseminate this document as Indicated above. Reproduction from the ERIC microfiche or electronic/optical media by persons other than ERIC employees and its system contractors requires permission from the copyright holder. Exception is made for non-profit reproduction by libraries and other service agencies to satisfy information needs of educators in response to discrete inquiries."

Sign here→ please

Signature: William L. Adkins	Printed Name/Position/Title: WILLIAM L. ADKINS SECRETARY/TREASURER
Organization/Address: CHECS 2701 CAMPUS BLVD., NE ALBUQUERQUE, NM 87131-6046	Telephone: (505) 277-8071 FAX: (505) 277-8101
	E-Mail Address: badkins@unm.edu Date: August 9, 1996

(over)